CONNECT.DC
Digital Inclusion Initiative • Powered by OCTO

CYBERSECURITY AWARENESS GUIDE

Version 1

October 3rd, 2019

CYBERSECURITY AWARENESS GUIDE

WE LIVE IN A CONNECTED WORLD

Computers and the Internet help us maintain our financial, social, and professional relationships.

We have a strong online presence—we use the internet for online banking, shopping, paying our bills, connecting with family and friends through email, Facebook, Twitter, SnapChat, Instagram, Google for information, looking for jobs and business opportunities, and so much more.

We use computers and mobile devices to use these services, yet we sometimes overlook our need to secure them and our information. So much of our personal information is online, and it does not go away easily.

WHAT IS CYBERSECURITY?

- Cybersecurity refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.

- One of the most challenging aspects of Cybersecurity is the ever-changing and evolving nature of security risks.

- Cyber Threats can be defined as the possibility of a malicious attempt to damage or disrupt a computer network or system.

WHAT IS PII?

- **Personally Identifiable Information (PII)** is any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources.

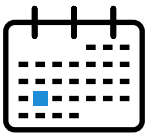
- It includes information that is linked or linkable to an individual, such as medical, educational, financial and employment information.

- Sensitive PII is information which, when disclosed, could result in harm to the individual whose privacy has been breached. It includes biometric information, medical information, personally identifiable financial information and passport or Social Security numbers.

Driver's License #

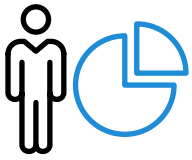
Passport #

Social Security #



Date/Place of Birth

Medical, Educational, Financial, Employment Info.



Biometric Info.

NOTES:

10 WAYS TO STAY SAFE WHILE BROWSING

1. Be Aware of Cyber Crime and Malware

Malware is malicious software code developed by cybercriminals to infect PCs, networks and mobile devices for the purpose of gaining access to and extracting sensitive data, typically for financial gain.

You are their #1 target. Whether you're using a PC at home or at work, you are just a tool for cybercriminals to gain access to the data they want to steal or the systems they want to hijack.

Some malware types, like viruses and Trojans, are tools for breaking into your PC. While others like worms, spyware and key loggers, are all about snooping through a PC or network looking for particular systems to compromise and data to steal.

Still other malware, like bots or bot nets, are all about hijacking PCs to steal computing resources to launch other cyber-attacks. Scammers often secretly use a network of infected PCs around the world to distribute malicious email without users ever knowing.

Did you know... There are more than 200,000 new malware threats created every day, and nearly 70% of data breaches involve malware.

Tip # 1

Don't underestimate how clever cybercriminals have become. Their tricks are extremely effective at luring users to open infected files, click on malicious links, unwillingly share malware with colleagues, and to freely divulge sensitive data. They understand how we behave online, and they know exactly what to do to infect us. Knowing the types of tricks and traps they use is the first step to defending yourself from malware.

NOTES:

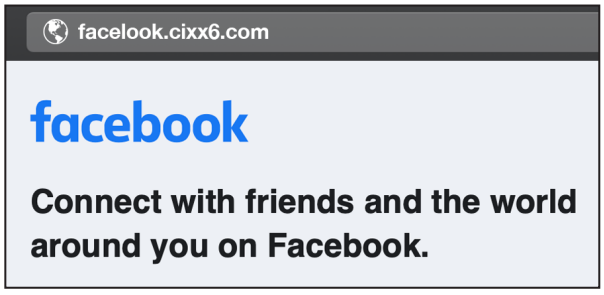
2. Don't Fall for Scams and Tricks

Believe it or not, one of the most common ways that cybercriminals gain access to sensitive data is by tricking users into divulging information they ordinarily wouldn't share with anyone.

It's called phishing, and it often involves using social engineering tactics to trick users into thinking they have been contacted by a service they know and trust like a bank, online retailer, airline or social media platform typically via a fraudulent email requesting that a user disclose sensitive information like passwords, credit card details and even social security numbers.

Social engineering refers to the practice of creating deceptive attacks based on what is known about the targeted user. For example, cybercriminals scour users' social media accounts like Facebook and LinkedIn to create phishing emails that look and read real enough to trick users into responding to fraudulent requests to change passwords, confirm payment options or divulge other personal information.

Phishing emails and the websites they link to look like the real thing and can be difficult to identify as malicious right away. It is common for many people re-use the same password for multiple accounts—a user's login credentials for a bank account is often the same one they use to log on to the network at work every day.



Does this Facebook link look real to you? It's not. It was part of a phishing campaign to steal passwords. It uses a false url to get users to login with their Facebook credentials.

Tip # 2

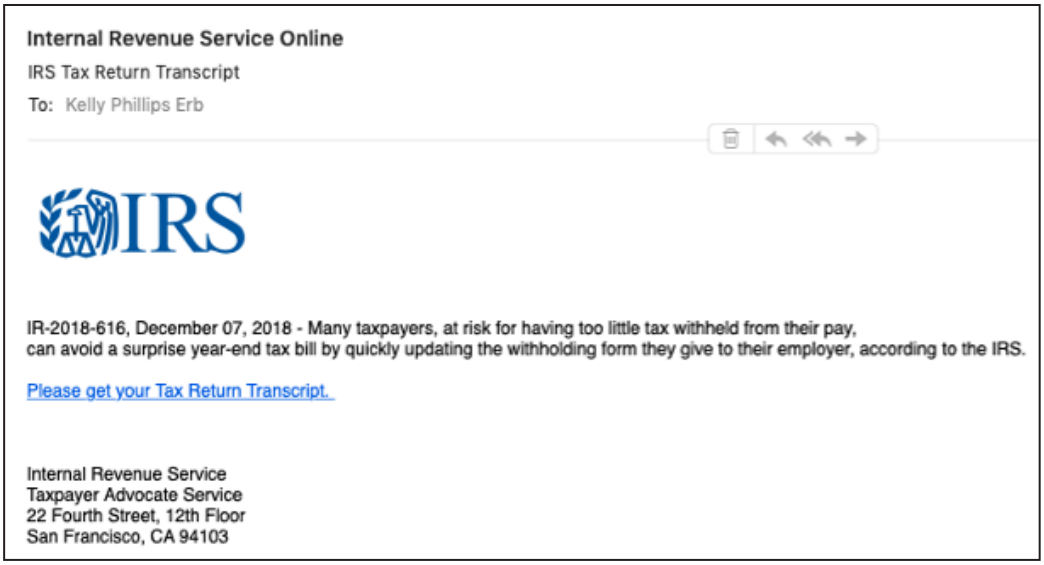
Always keep in the mind that most of the services you use will never request that you share personal information directly via email. Moreover, the majority of time you are contacted to reset a password or confirm any changes to your account will be initiated by an action you take. Almost all unsolicited email should be assumed to be malicious. Do not click any links. Contact the service provider or check their website by entering the URL you always use.

3. Resist Your Curiosity

Malicious spam remains a major threat to both the user and businesses. These aren't those annoying marketing emails we're tired of deleting from our inboxes all day long. Think of malicious spam as a precursor to phishing, employing similar tricks of deception, stealing logos and designs from well-respected brands, to trick users into clicking malicious links or downloading infected files.

Malicious spam could even come from an email address spoofed (manipulated) to appear as if it is from someone you know. But one click of the mouse to open an infected Word document or PDF, and your PC may be infected.

Just about any type of malware can be delivered via malicious spam. Often these emails are disguised as shipping confirmation notices, alarming notices from banks, tantalizing photos, mortgage scams, fake news alerts and more—anything to raise our curiosity and get us to open an email and click an attachment or link that only leads to trouble.



Tip # 3

Always be wary of any email you receive that is out of the ordinary or you did not request. Spam can look very real, but avoid the temptation to click without thinking. If you think it's spam, delete it.

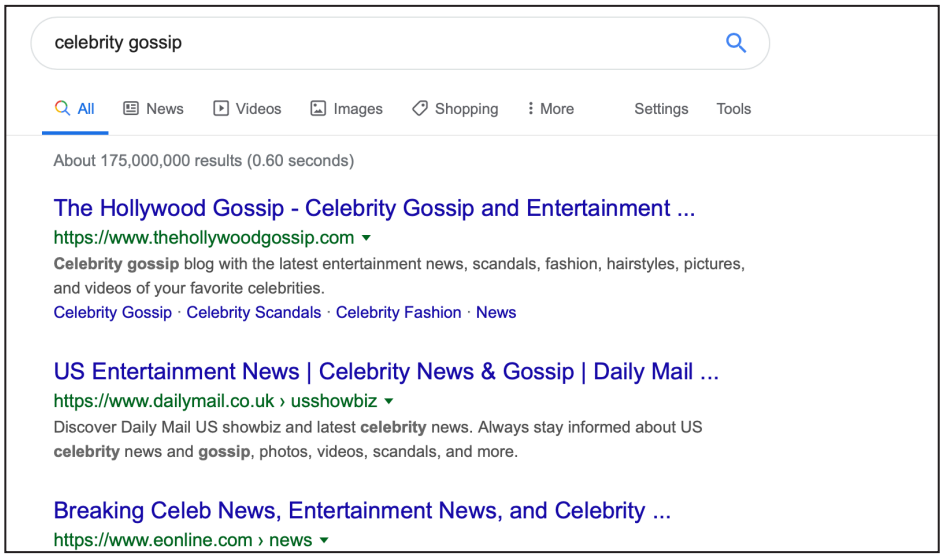
NOTES:

4. Browse with Care

A favorite trick of cybercriminals is to poison internet search results. Cyber criminals use our curiosity against us by exploiting high-profile events like a celebrity scandal, new tech gadget or major events like the Olympics, an election or sports championship.

Cybercriminals know what people are searching for online and talking about via social media, and use that information to develop fake sites within hours of sensational news breaking to deliver malware.

While search engines like Google are very good at protecting us from these threats, it may take Google a few hours to identify and remove these sites from its search results, but in that time plenty of users can be infected.



Tip # 4

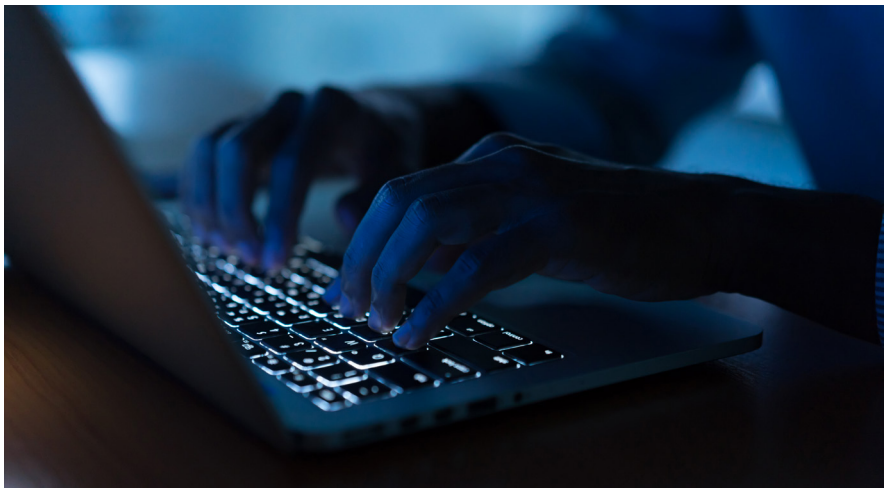
Get your celebrity gossip and news from trusted sites only. Always be careful what you're searching for and what sites you visit on your lunch hour. Again, don't assume you're protected because work has better security than your home PC. Threats, especially newly created threats, can still slip through.

NOTES:

5. Don't Get Exploited

Two types of malware known as exploits and Zero-day attacks refer to cybercriminals taking advantage of vulnerabilities in the software products we use every day. These include operating systems like Windows, web browsers like Chrome, Internet Explorer and Firefox, and a wide range of popular applications like Adobe Flash and Reader, Java and Skype.

Hackers invest a lot of time and energy searching for faulty software code they can exploit and use as a backdoor into your PC to deliver malware for any number of malicious purposes. Zero-day attacks are named as they are because at the time of their discovery there is no fix for the vulnerability they are exploiting, leaving software companies scrambling to release updates within a few days, which is plenty of time for cybercriminals to spread malware.



Tip # 5

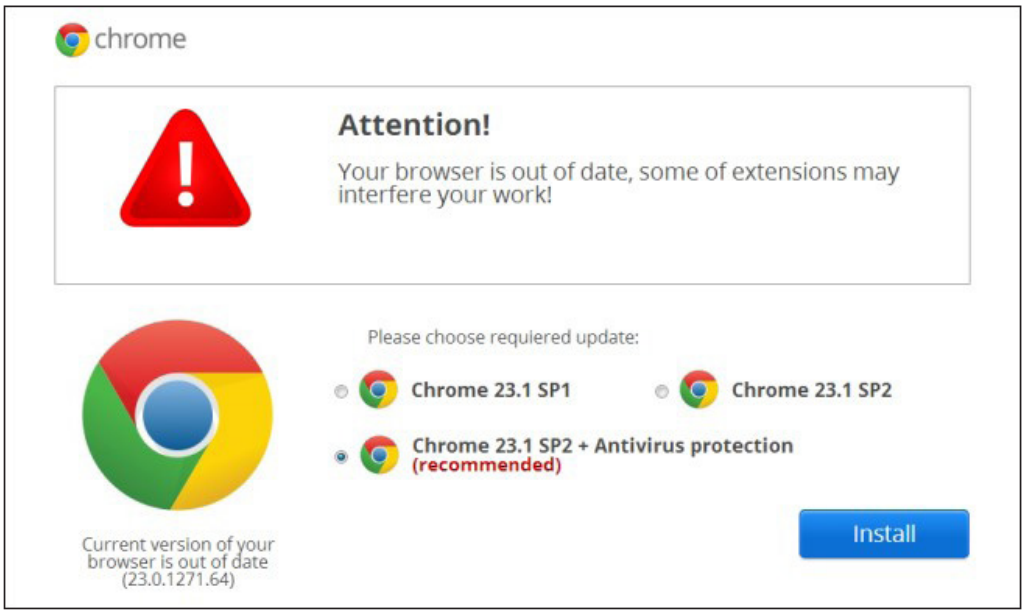
The best defense against malware exploits is to always update software programs to the latest available versions. When a message appears on your screen to update a trusted software application, do it. Chances are good the software developer is correcting an issue that may have serious security implications. Browsers like Google and Chrome automatically update the software the next time the browser is restarted, while Microsoft uses patch notifications.

NOTES:

6. Don't Be Click Happy

Cybercriminals know that users are concerned about security and often employ messages and pop-up screens that appear to be legit programs on your PC requesting updates. Clicking on these links can lead to downloading malware and installing rogue applications.

These rogue software may claim to be antivirus products or system cleaning programs. Some even claim to be from the FBI. They look authentic, but they are designed to infect your PC to extort money from you, or to install additional malware on your computer.



Tip # 6

If you see a warning claiming your PC is infected, don't click anything. Contact a Computer Professional. Don't take the chance.

NOTES:

7. Back It Up

There is a family of malware known as ransomware, and just like the name implies, these malicious programs take your PC hostage. By clicking on the wrong link in an email or by visiting an infected website, your PC can fall victim to malware that demands payment to be removed, or even worse large sums of money to regain access to your files. Hijacking users' PCs and encrypting files so they are no longer accessible is an increasingly popular tool in the bad guys' arsenal.

Tip # 7

Avoid ransomware by being safe online, but be prepared for the worst and back up all critical files your business or operation can't do without. And since ransomware is often delivered via malware exploits, keep your system patched and software up to date.

NOTES:

8. Stay Safe While Mobile

Malware is no longer limited to just PCs. With the rise of mobile devices and their proliferation in the workplace, hackers have switched tactics to take advantage of these inviting targets. Malicious Android and iOS apps can cause all sorts of headaches – from running up international text charges to stealing personal data and passwords to transmitting infections to other devices, like your PC.

In September 2010, more than 1 million cell phones in China were infected with a virus that continually sent out text messages.

Tip # 8

Don't think that your Android or iOS device is safe from threats. Mobile malware is the fastest growing segment of malware. When downloading apps, only download from trusted sources (Google Play and Apple's App Store) and only choose apps from trusted developers. Moreover, install a trusted security app onto your mobile device.

NOTES:

9. Don't Be a Carrier

Just like people can spread the flu or a cold to colleagues, users can spread malware infections to their work PC and network. Two common ways this happens is by sharing files between a work and home PC that may not be as secure or is used by other family members who do not practice safe online habits.

Users may work on an infected document on their home PC and email it to their work computer or upload to the cloud where other users may access it, getting infected themselves. Sharing devices between users is also risky as this can carry a virus from one machine to another resulting in multiple infections.

Phishing emails and the websites they link to look like the real thing and can be difficult to identify as malicious right away. It is common for many people re-use the same password for multiple accounts—a user's login credentials for a bank account is often the same one they use to log on to the network at work every day.

Tip # 9

Only connect your PC to trusted devices and scan all USB drives with your antivirus software before opening any files. Be mindful of who is using a home PC if you are opening work documents on it.

NOTES:

10. Know Your Friends

Security threats on social media continue to grow exponentially. Shortened links are effective tools to hide malicious URLs, and threats tied to compelling images and videos shared on Facebook can spread quickly among friends.

Cybercriminals can quickly set up fake accounts and profiles to spread malware, typically employing the same social engineering tactics they've perfected. Moreover, cybercriminals can hijack your profiles and accounts to spread malware under your name to people you're connected to.

Tip # 10

Be careful what you click on Facebook, Twitter, Linkedin and other popular social channels. Only share and click on posts from trusted sources, and be mindful that it's possible your friends are sharing malware. Also, use different passwords for all your accounts, so if one is compromised the others are still secure.

NOTES:

HOW TO SECURE YOUR HOME NETWORK

It is important to use good security practices when you configure devices in your home network.

1. Configure and Connect to a Secure Network.
2. Enable and Configure a Firewall.
3. Install and Use Antivirus and Antispyware Software.
4. Modify unnecessary default features from desktop machines and laptops.
5. Operate under the Principle of Least Privilege. Only use administrator privileges when installing new applications or running updates.
6. Secure Your Web Browser.
7. Remove Unnecessary Software.
8. Apply Software Updates and Enable Future Automatic Updates.
9. Use strong passwords.

NOTES:

DO'S AND DON'TS OF ONLINE SHOPPING

While shopping online is popular and convenient, here are some tips before you click "buy." Remember, never click on links attached to an unsolicited email.

Do:

Do check with your parents to make sure it's ok for you to shop online if you are a minor.

Do check Internet merchants' refund policies; some merchants set a deadline for returns or charge a fee to accept returned merchandise.

Do keep in mind you often pay shipping fees to have your purchases delivered.

Do make sure your computer has the latest anti-virus software installed.

Do print and save the confirmation page (your receipt) when completing an online purchase.

Do be responsible. Remember, once you make a transaction online you have legally committed to purchasing that item.

Don't:

Don't share your passwords with anyone.

Don't wait for paper statements. Check your credit card and bank statements regularly for suspicious activity.

Don't respond to unsolicited email or pop-up ads. Shop only at websites you know and trust. Look for "https" at the beginning of the web site address - "s" means secure.

Don't provide merchants with personal information such as your Social Security number, birth date, or mother's maiden name.

Don't get drawn in by emails offering cheap deals on popular items and gifts. If the offer sounds too good to be true, it probably is.

Don't use your debit card to make purchases. Instead, use a credit card. Getting a fraudulent charge reversed on your credit card is infinitely less stressful than restoring a balance to your checking account.

CYBER TIPS FOR PARENTS

- Engage with your kid's online activities.
- Support their good online choices.
- Keep a clean computer using regular updates and antivirus software.
- Know the protection features of the websites and software your children use.
- Review privacy settings of online applications.
- Teach critical thinking skills to identify appropriate and safe digital content.
- Explain the implications of the public nature of the internet and sharing personal information.
- Help them be good digital citizens by respecting others.
- Explain consequences of cyber-bullying and how to handle hurtful comments.
- Remind them not to share personal information with new acquaintances.

NOTES:

TEEN SAFETY TIPS

- Share With Care.
- Personal Information Is Like Money. Value It. Protect It.
- What you post can last a lifetime: Before posting online, think about what others might learn about you and who might see it in the future; teachers, parents, colleges and potential employers. Share the best of yourself online.
- Be aware that when you post a picture or video online, you may be sharing information about others like where you live, go to school or hang out.
- Post about others as you would like to have them post about you. Ask permission before you tag a friend.
- Own your online presence: It's OK to limit who can see your information and what you share. Learn about and use privacy and security settings on your favorite online games, apps and platforms.

NOTES:

CYBER TIPS FOR SENIORS

There are risks associated with being online, and, sadly, many scammers target senior citizens. Older citizens should be wary of the following types of emails, websites, or social media messages that:

- Offer "free" gifts, prizes or vacations, or exclaim, "You're a winner!"
- Offer discount prescription medications or "can't miss" deals.
- Appear to be from friends or family members, but the message is written in a style not usually used by that person, has numerous misspellings, or otherwise seems unusual. This is an indication your friend or family member's account may have been hacked.
- Appear to be from official government agencies, such as Social Security Administration, or banks, requesting personal information.
- Set ultimatums such as "your account will be closed," or "the deal will expire" to create a sense of urgency, and trick the victim into providing personal information.

NOTES:

CYBER BULLYING OF SENIOR CITIZENS

Though there is a lot of focus on cyberbullying among children and teens, cyberbullying affects senior citizens as well. Cyberbullying (mostly through e-mail) of seniors can take several forms, but the most common are:

- **Emotional abuse with rage, threats, accusations, and belittling comments, often followed with periods of silence or ignoring the victim.**
- **Financial abuse aimed at obtaining the victim's account information, setting up online access to their accounts, and stealing their money.**

Speaking out against cyberbullying can be particularly difficult for seniors who may not even know what the term means.

As with victims of any age, seniors may feel violated and powerless, be confused and in denial over what's happening, feel shame and self-blame for being a victim, and fear even more bullying or being ignored if they speak out.

Additionally, according to the Washington State Office of the Attorney General, in many cases, seniors are the victims of cyberbullying by family members.

CYBER AWARENESS

WHY SHOULD YOU CARE?

Somewhere out in cyberspace there is a hacker, attacker or individual with malicious intent who would like to harm, steal, access, sell, and/or disrupt your computer system, website and/or electronic data.

It is no longer wise to think that nobody is interested in your computers, network or data, because you are too small or don't have anything of value to steal. History has shown that cybercrimes sometimes affect the most unlikely victims.

octo

GOVERNMENT OF THE DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR